UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/495,157	01/31/2000	Thomas D. Ashoff	NAI1P075/99.039.01	4471

7590 09/10/2003

Schwegman, Lundberg, Woessner & Kluth, P.A.
P.O. Box 2938
Minneapolis, MN 55402

EXAMINER
MASHAAL, ALI M

ART UNIT	PAPER NUMBER
2133	10

DATE MAILED: 09/10/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/495,157	ASHOFF ET AL.	
	Examiner	Art Unit	
	Ali M. Mashaal	2133	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2000* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☒ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Oath/Declaration

1. The oath or declaration is defective. A new oath or declaration in compliance with 37 CFR 1.67(a) identifying this application by the application number and filing date is required. See MPEP §§ 602.01 and 602.02.

The oath or declaration is defective because:
The "[ ] is attached to option is marked, when in fact the declaration was filed after the application, and therefore could not have been attached.

Specification

2. The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. For example on page 4, lines 11 and 12, "http://www.stanford.edu/~hodges/talks/mactivity.ldap.97/index2.html". Applicant is required to delete **all** embedded hyperlinks and/or other forms of browser-executable code. See MPEP § 608.01.

Drawings

3. Figures 1, 4, and 5 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 1-7 are rejected as being directed to non-statutory subject matter.

Claim 1 is directed to a system for authorizing client access. However, the system comprises a directory, firewall, and authorization filter. As mentioned on page 2 of the Specification, a firewall can be software alone, see lines 10-12. The directory, asserted in figure 4, is a collection of data. The filter is the criteria used for authentication and is intangible; see page 11, lines 7-10, and page 14, lines 15 and 16. Each of the components in claim 1 is disclosed as being implemented as software alone with no tangible elements.

Claims 2-7 each further limit claim 1 by adding an intangible feature as disclosed below.

Claim 2 limits claim 1, only to specify an LDAP directory and therefore is rejected over claim 1.

Claim 3 limits claim 1, only to specify the filter using a GUI and therefore is rejected over claim 1.

Claims 4 and 5 limit claim 1, only to specify the implementation of a per-user and per-service scheme respectively, and therefore are rejected over claim 1.

Claim 6 limits claim 1, only to specify SSL as the protocol for communication between the firewall and the directory, and therefore is rejected over claim 1.

Claim 7 limits claim 1, only by specifying multiple directories and therefore is rejected over claim 1.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over US patent number 6,131,120 to Reid in view of The Microsoft Computer Dictionary, 1997, further in view of Check Point Account Management Client, Version 1.0, September 1998.

7. In reference to claims 1, 8, and 17, Reid substantially discloses a system comprising at least one directory, column 5, lines 23-31, that can be accessed using a network protocol. Although not explicitly mentioned, the only possible way for the directory to communicate with the various components on the network illustrated in figure 4, is through the use of a network protocol.

Column 5 lines 23-35 and column 6 lines 54-65, discuss the possibility of deleting or omitting a firewall and implementation of the firewall functions into other network elements. However, the examiner first notes that per the Microsoft Computer Dictionary, a firewall is defined as a security system intended to protect an organization's network against external threats; a firewall prevents computers in the organization's network from communicating directly with computers external to the network and vice versa. In Reid, the firewall functions are integrated into a router/gateway receiving information (Router Access List) from a directory server, see column 6 lines 17-26 and lines 57-61. Acting as the firewall, the routers/gateways

download the access list, and grant or deny access correspondingly. The examiner asserts that while the reference teaches elimination of a separate firewall, it does not in fact eliminate the firewall altogether but instead combines the functions of a firewall with that of a router/gateway into a single unit.

This firewall is configured to intercept network resource requests, see Reid, column 8, lines 6-11, which outlines that the users are either allowed or denied access by the router/gateway. This means that the router/gateway intercepts the users network requests.

Also, column 8, line 9, says "each user" in reference to users accessing the WAN. This establishes a plurality of users.

As per comparison of the authorization filter to directory entries, the examiner asserts that normal and well-known function of a firewall is to selectively control what client user has access to resources it protects. Thus, some type of authorization filter (i.e. filter relative to authorization information) would have to be executed. In Reid, see column 8 lines 14-21, RAL, or router/gateway access list is sent to each router/gateway and controls who may have access through router/gateway. The examiner asserts that in order for the directory to generate the appropriate access list, each router/gateway must have transmitted its access criteria to the directory. The examiner further asserts that this criteria is an authorization filter and that in order for the directory to send back a correct access list, some comparison must have been made with directory entries and the router/gateway criteria (authorization filter).

As per the filter being generated based on schema that is predefined by the entity, Reid discloses that the access list is all ready set in the master directory and is then downloaded to the router/gateway, column 8, lines 14-21. This asserts that the schema is predefined, and that the filter is generated based on it.

We have established to this point that Reid teaches a system for authorizing client access to a network resource having one or more directories that can be accessed through a network protocol, and a firewall that is configured to intercept network resource requests from a plurality of clients, in which the firewall authorizes the requests of the clients based on one or more entries in the said directory to an authorization filter, wherein the authorization filter is generated based on a directory schema that is predefined by the said entity.

As per the directory being configured to store information concerning an organization's entity, Reid's directory, is configured to store names, workstations, router/gateways, servers, IP addresses, locations and so on, column 5, lines 36-39. Reid's directory does not store information concerning an entity's organization. Check Point Account Management Client (disclosed in applicants IDS) teaches storing an entity's organization in a directory tree, page 2, figure 1-1 LDAP Tree Example. Since this structure can be used to authenticate users, it would have been obvious to one of ordinary skill in the art at the time of the invention to take the analogous storage directory tree of Reid and modify it such that Reid's directory tree stored an entity's organization similar to that if Checkpoint. Examiner also notes that Reid implies that it is not necessarily true that what he chooses to store in the directory is the only thing

that can be stored, refer to column 7 line 61, when Reid says "In the embodiment of this invention, the objects may be individual's names....".

8. In reference to claims 2 and 9 which further limit claims 1 and 8 respectively by specifying the directory as being an LDAP directory, Reid teaches a system analogous to that in claims 1 and 8 as mentioned above, and also teaches the use of LDAP directories. See column 4, lines 7-11, column 6, lines 20-24, and column 8, lines 28-31.

9. In reference to claims 4 and 5, which each depend from claim 1, Reid substantially teaches a system analogous to that in claim 1 as mentioned above, and also teaches that the directory contains objects with associated attributes. Specifically, Reid says that the users, router/gateways, and servers are objects. The examiner asserts that Reid's invention teaches both per-user and per-server authentication since this object-oriented directory is organized such that users, router/gateways, and servers are all objects each of which having attributes that include IP address, password, privileges, and location. See column 6, lines 13-20. Accordingly, Reid substantially suggests that any of the two authentication methods could be used.

10. Claims 6 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reid as applied to claims 1 and 8 above, and further in view of US patent number 5,657,390 to Elgamal. Reid's invention fails to teach the use of SSL as means to secure the communication between the firewall and the directory. Elgamal's analogous

invention teaches that because the socket layer is widely used in networks, integration of SSL into machines that are connected to the network and receive requests would be facilitated. See column 1, lines 60-63. It would have been obvious to one having ordinary skill in the art at the time the invention was made to take Reid's firewall and use the SSL method taught by Elgamal to communicate between the firewall and the directory. One having ordinary skill in the art at the time the invention was made would have been motivated to do so because Elgamal establishes a need for SSL as a security mechanism between various applications to transfer various data between one another. See column 1, lines 44-54. Furthermore, the nature of the information being transferred between the firewall and the directory in the applicant's invention is private and sensitive.

11. In reference to claims 7 and 14, which further limit claims 1 and 8 respectively by specifying multiple directories being queried, Reid substantially teaches a system analogous to that in claims 1 and 8 as mentioned above, and also teaches the use of multiple directories as described in column 7, lines 58-61, when he refers to distributed directories and a master directory.

12. In reference to claims 15 and 16 which further limit claim 8 by specifying that the request comes from an internal user and an external user respectively, Reid substantially teaches a system analogous to that in claim 8 as mentioned above, and also states that his system handles both internal and external requests. Refer to

column 7, lines 39-44, when Reid says that the security policy is defined whether the user is internal or external to the network.

13. Claims 3 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reid as applied to claims 1 and 8 above, and further in view of US patent number 5,898,830 to Wesinger. Reid discloses a system that encompasses all the limitations of claims 1 and 8, but fails to teach the use of a GUI interface to specify the authorization filter. Wesinger, in an analogous art, teaches the use of a graphical user point and click web interface for configuring the firewall and specifying configuration parameters. It would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the firewall of Reid to include a GUI interface by which the authorization filter could be specified. One having ordinary skill in the art at the time the invention was made would have been motivated to do so because graphical user interfaces have become highly popular and favored for their ease of use, and because they are cheap and easy to develop.

14. Claims 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Reid in view of Wesinger as applied to claims 3 and 10 above, and further in view of Reid as applied to claims 4 and 5 above.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The following patents are cited to further show the state of the art with respect to directory-based access controlled networks:

U.S. Pat. No. 006047322A to Vaid

Pub. No. 20030126468 to Markham

U.S. Pat. No. 006212558B1 to Antur

U.S. Pat. No. 006233688B1 to Montenegro

U.S. Pat. No. 006324648B1 to Grantges

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ali M. Mashaal whose telephone number is 703-305-7854. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3800.

A M

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

09/04/03